警惕落入『网络窃密圈套』 轻轻松松就能赚钱？

近年来，信息科技高速发展，为人们生活带来了便利，但同时也让一些新的“危险”悄悄潜伏在了我们身边。从国家安全机关破获的多起案件看，境外间谍情报机关利用网络实施“障眼法”，在眼花缭乱的虚拟空间里对我境内人员进行“钓鱼”，从而窃取我国家秘密的情况屡见不鲜，给我国家安全带来严重威胁。虽然相关人员已被绳之以法，但这些典型案件也警醒我们提高警惕，不要落入境外间谍情报机关精心布置的“网络窃密圈套”！

精心“包装”的电子谎言

某政府机关工作人员小何因欠外债经济压力过大，主动登陆浏览境外某网站，并加入诸多群组，寻求赚钱渠道。

在一次网聊中，小何结识了一名自称研学机构的人员“小静”。在了解到小何拮据的经济状况后，“小静”表示，只要小何提供一些单位内部资料，就可以轻轻松松赚取“外快”。面对“小静”开出的高价，小何开始频繁拷贝并私自留存各类单位内部培训课件、偷拍办公室的涉密文件、挖空心思寻找内部讲话材料，并按照约定时间发送给“小静”。

为了诱导小何继续获取更多有价值的涉密材料，“小静”还奖励了小何一个“大红包”。在金钱和利益的不断驱使下，小何逐渐迷失自我……

很快，小何的异常行为引起了国家安全机关的注意。

经过调查，小何一共向境外非法提供涉密文件资料近30份，违法获利6万余元，而“小静”的真实身份，则是境外间谍情报机关人员。2022年6月，小何因涉嫌为境外窃取、非法提供国家秘密罪被批准逮捕。最终，小何被依法判处有期徒刑十年。

网络窃密的常见“套路”

境外间谍情报机关人员及其代理人往往会在网络上为自己伪造一个虚假身份，以此来包装其对国家秘密或敏感信息需求的“合理性”，然后利用互联网上各种交友、求职网站及软件，发布虚假的岗位招聘、兼职或交友等信息，对我境内人员进行拉拢、渗透和策反。

寻猎的惯用虚假身份：

某杂志社的编辑或记者、某学院的研究人员、某公司的技术开发人员、某咨询公司顾问、某领域的爱好者、商人等。

寻猎的常用网络平台：

互联网论坛、短视频平台、社交平台。

寻猎的重点目标对象：

科研人员、政府机关工作人员、敏感场所服务人员、高校师生等。

网络防范要有“三个心”

网络空间纷繁复杂，境外间谍情报机关人员及其代理人十分擅长伪装，具有很强的迷惑性，要想远离“网络窃密陷阱”，务必提升网络安全防范意识，做到“三个心”：

网络交友要“小心”。

首先可以通过IP地址、聊天惯用语、语法等判断对方是否为境外人员，对于境外IP、使用非简体中文或翻译器等情况的人员提出的“提供兼职”“寻找资料”等相关要求，一定要保持警惕，认真判明其真实意图。

公开发布要“留心”。

在互联网社交平台公开发布的言论和照片时，要留心是否包含涉及个人敏感信息等内容，万万不可发布涉及国家秘密的内容，否则很可能被境外间谍情报机关人员盯上进而“围猎”。

稿费报酬莫“贪心”。

对于陌生人许诺的稿费酬劳等不要贪心，对于一些明显超出正常范畴的报酬更要小心辨别。看似“泼天的富贵”，其实正是拉人“下水”的陷阱。一旦迈出泄密的“第一步”，就有可能陷入为境外刺探、非法提供国家秘密、情报的犯罪深渊，无法自拔。

国家安全机关提示

《中华人民共和国反间谍法》规定，间谍组织及其代理人实施或者指使、资助他人实施，或者境内外机构、组织、个人与其相勾结实施的危害中华人民共和国国家安全的活动，属于间谍行为。

维护国家安全是每个公民的责任与义务，如发现危害国家安全的违法行为及可疑线索，请及时通过12339国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或直接向当地国家安全机关进行举报。

警惕云存储泄密风险

云存储是一种新兴网络存储技术。近年来，随着网络“云”功能不断普及，“云端”数据也成为了境外间谍情报机关关注的重点，他们通过网络攻击、植入木马等各种手段，试图窃取我敏感信息和涉密数据，给个人隐私和国家安全造成严重威胁。一些单位和个人为图方便快捷，将敏感信息或涉密事项上传至“云端”，造成相关敏感涉密信息数据在互联网上“裸奔”，给境外间谍情报机关网络窃密带来了可乘之机。

“云”上存储需脱密

近年来，国家保密行政管理部门公布了多起违规云存储国家秘密的案例，相关责任人在未经保密审查的情况下，将涉密资料上传至网络，事后均依纪依法受到严肃问责处理。

比如，某省直单位工作人员李某，利用自己的网盘私自保存机密级涉密资料。

比如，某县级机关工作人员杨某为方便工作，擅自将收集到的包括1份机密级文件、2份秘密级文件在内的大量文件资料上传至某网盘，并回家下载使用。

比如，某县领导干部方某，在未经保密审查的情况下，要求办公室工作人员将包含1份秘密级文件在内的15份文件材料上传到某网盘，并设置为分享模式，供有关人员浏览。

上述案例反映出，使用者保密意识淡薄、侥幸心理作祟是导致云存储失泄密的重要原因。党政机关和涉密单位工作人员应始终绷紧保密之弦，规范使用互联网行为，严禁通过网络、手机、云盘等存储、处理、传输、谈论涉密及敏感信息，坚决防范失泄密事件发生，确保国家秘密安全。

“云”端防护需加强

在日常工作生活中使用互联网处理个人事务时，面对云存储账户易遭非法网络攻击等风险，需从操作层面加强相应安全防护。

严禁涉密信息上网。

相关人员和单位应坚守“涉密不上网、上网不涉密”底线，严禁通过互联网上传、存储、处理涉密信息，严守国家秘密和工作秘密。

做好敏感信息保护。

个人隐私或敏感信息，尽量不要上传至“云端”，如果必须上传，可将重要信息设置为“禁止分享”。敏感信息通过U盘、光盘等与外界有物理隔离的介质进行备份。

进行网盘内容加密。

目前，大多数云存储网盘都提供文件加密功能，对于需要分享的云存储数据，建议设置“提取码”，并设置“分享时效”，减小信息泄露的可能性。

及时维护账号密码。

将账号与手机、微信、邮箱等绑定，登陆时通过动态验证码进入；设置较为复杂的密码，并经常修改密码，发现账号异常时及时调整密码。

谨慎选择“自动备份”。

很多服务商为用户提供将照片、通讯录、数据等信息定期自动备份到“云端”的功能，建议慎重选择该功能，可通过手动方式，有选择地对相关数据进行备份。

国家安全机关提示 >>>

《中华人民共和国保守国家秘密法》规定，禁止未按照国家保密规定和标准采取有效保密措施，在互联网及其他公共信息网络或者有线和无线通信中传递国家秘密。

《中华人民共和国数据安全法》规定，利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行数据安全保护义务。

网络化、数字化、智能化时代，广大人民群众和相关单位要提高保密意识，强化保密观念，履行保密义务，落实保密责任，坚决筑牢新时代维护党和国家秘密安全的坚固防线。国家安全机关将在党中央坚强领导下，与有关部门协同配合，坚决维护国家网络安全、数据安全。

（均转自国家安全部微信公众号）

责任编辑：王睿卿 E-mail: fzbfyzk@126.com